Virus - The truth is out there

Éric BERTHOMIER
berthomiereric70@gmail.com

4 janvier 2026

Version 1.1 - Version Stagiaire

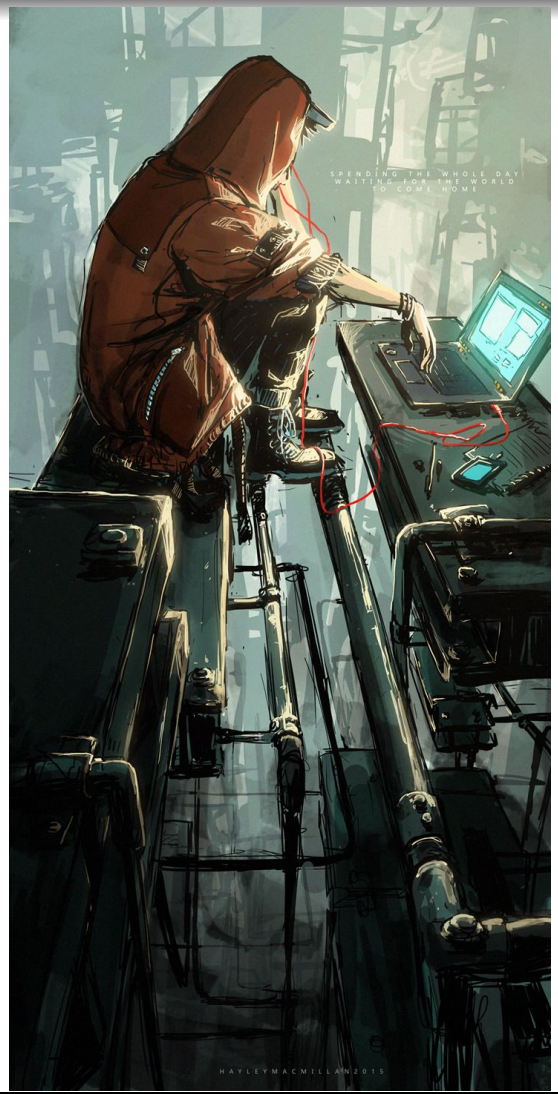
Fil conducteur

Sun Tzu - Art of war

Si vous connaissez l'ennemi et que vous vous connaissez vous-même, vous n'aurez pas à craindre le résultat de cent batailles.

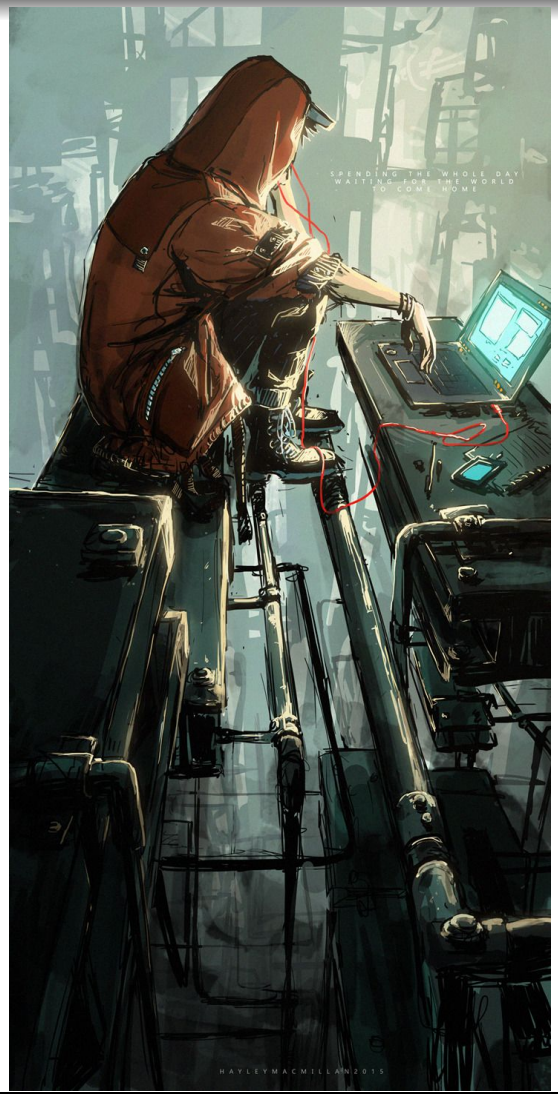
Si vous vous connaissez vous-même mais pas l'ennemi, pour chaque victoire remportée, vous subirez également une défaite.

Moi



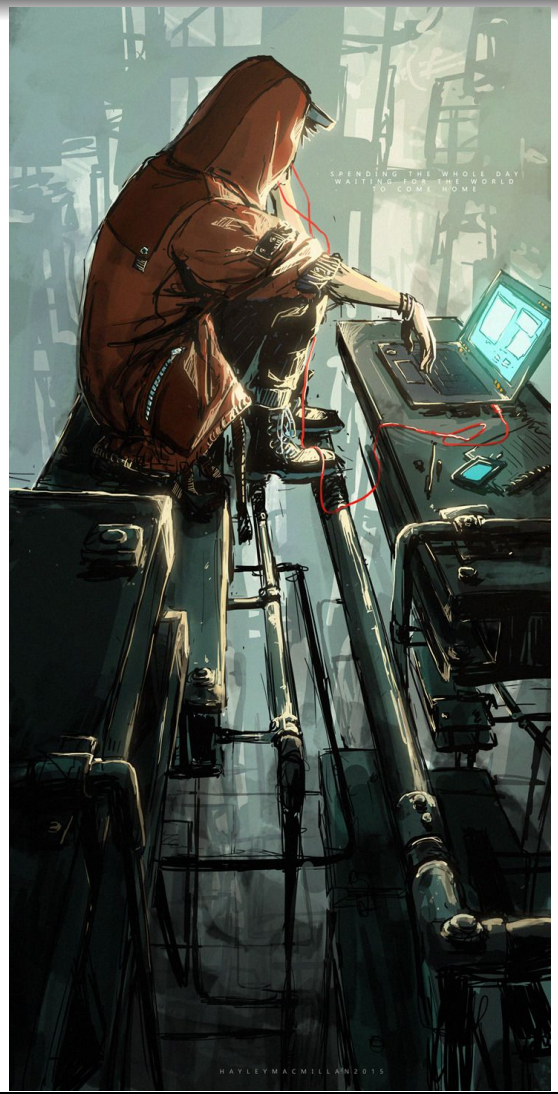
- Profession :
  Analyste cyber

Moi



- Profession :
  Analyste cyber
- Forces / faiblesses :
  Esprit de compétition
  Passionné
  ...

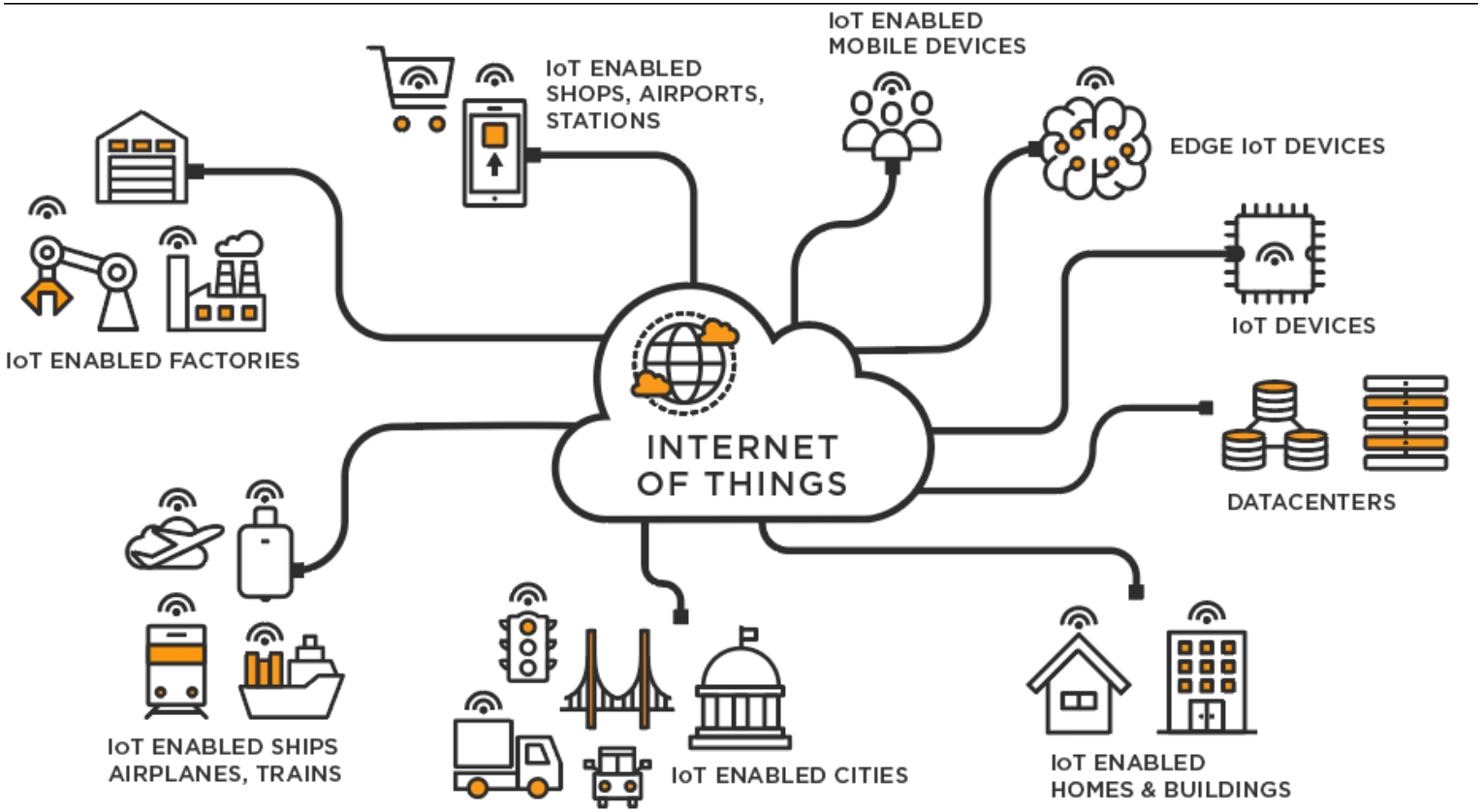
Moi



- Profession :
  Analyste cyber
- Forces / faiblesses :
  Esprit de compétition
  Passionné
  ...
- Citation :
  The quieter you become, the more you are able to hear.

Notre environnement

On nomme Internet of Things (IOT), tout objet connecté à Internet.



Nos besoins mathématiques

Question :

Combien existe-t-il de méthodes mathématiques pour obtenir la valeur 104 ?

Nos besoins mathématiques

Question :

Combien existe-t-il de méthodes mathématiques pour obtenir la valeur 104 ?

Réponse

Une infinité.

Notre besoin informatique

- I LOVE YOU

Notre besoin informatique

- I LOVE YOU
- Se traduit en ASCII par : 73 32 76 79 86 69 32 89 79 85

Notre besoin informatique

- I LOVE YOU
- Se traduit en ASCII par : 73 32 76 79 86 69 32 89 79 85
- Et peut donc s'écrire :

Notre besoin informatique

- I LOVE YOU
- Se traduit en ASCII par : 73 32 76 79 86 69 32 89 79 85
- Et peut donc s'écrire :

Notre besoin informatique

- I LOVE YOU
- Se traduit en ASCII par : 73 32 76 79 86 69 32 89 79 85
- Et peut donc s'écrire :

$$(7*10+3) \quad (50+19)$$
$$(128/4) \quad (8*2*2)$$
$$(12*6)+4 \quad (11*8)+1$$
$$(37*2)+5 \quad 5+(37*2)$$
$$(59*1)+27 \quad (170/2)$$

Notre besoin informatique

- I LOVE YOU
- Se traduit en ASCII par : 73 32 76 79 86 69 32 89 79 85
- Et peut donc s'écrire :

$$(7*10+3) \quad (50+19)$$
$$(128/4) \quad (8*2*2)$$
$$(12*6)+4 \quad (11*8)+1$$
$$(37*2)+5 \quad 5+(37*2)$$
$$(59*1)+27 \quad (170/2)$$

Question :

Quel est le rapport avec une signature d'antivirus ?

Notre besoin informatique

- I LOVE YOU
- Se traduit en ASCII par : 73 32 76 79 86 69 32 89 79 85
- Et peut donc s'écrire :

$$(7*10+3) \quad (50+19)$$
$$(128/4) \quad (8*2*2)$$
$$(12*6)+4 \quad (11*8)+1$$
$$(37*2)+5 \quad 5+(37*2)$$
$$(59*1)+27 \quad (170/2)$$

Réponse

Signature antivirale statique

Base de signatures des antivirus

Une signature de virus est un ensemble **unique** de données, de motifs ou de comportements caractéristiques permettant d'identifier un logiciel malveillant (malware) spécifique.

Base de signatures des antivirus

Une signature de virus est un ensemble **unique** de données, de motifs ou de comportements caractéristiques permettant d'identifier un logiciel malveillant (malware) spécifique.

- **Signature statique :** basée sur un extrait de code spécifique d'un virus connu.

Base de signatures des antivirus

Une signature de virus est un ensemble **unique** de données, de motifs ou de comportements caractéristiques permettant d'identifier un logiciel malveillant (malware) spécifique.

- **Signature statique :** basée sur un extrait de code spécifique d'un virus connu.
- **Signature heuristique :** détecte des comportements suspects plutôt qu'un code exact.

Base de signatures des antivirus

Une signature de virus est un ensemble **unique** de données, de motifs ou de comportements caractéristiques permettant d'identifier un logiciel malveillant (malware) spécifique.

- **Signature statique :** basée sur un extrait de code spécifique d'un virus connu.
- **Signature heuristique :** détecte des comportements suspects plutôt qu'un code exact.
- **Signature comportementale :** analyse le comportement d'un programme en temps réel pour repérer des actions typiques des malwares.

Cyberattaque

- Une cyberattaque **non ciblée** est une action malveillante menée de manière indiscriminée, sans viser une cible spécifique.

Cyberattaque

- Une cyberattaque **non ciblée** est une action malveillante menée de manière indiscriminée, sans viser une cible spécifique.
- Une cyberattaque **ciblée** est une action malveillante dirigée spécifiquement contre une organisation, une entreprise ou un individu particulier.

Détection

Un malware n'est déclaré en tant que tel qu'à partir du moment où un ensemble de personnes ont indiqué que ce programme réalisait des choses qu'il ne devrait pas.

Détection

Un malware n'est déclaré en tant que tel qu'à partir du moment où un ensemble de personnes ont indiqué que ce programme réalisait des choses qu'il ne devrait pas.

Ce dernier peut donc dormir au sein de votre ordinateur / smartphone / tablette / montre connectée... tant qu'un antivirus n'a connaissance de sa malveillance.

Détection

Un malware n'est déclaré en tant que tel qu'à partir du moment où un ensemble de personnes ont indiqué que ce programme réalisait des choses qu'il ne devrait pas.

Ce dernier peut donc dormir au sein de votre ordinateur / smartphone / tablette / montre connectée... tant qu'un antivirus n'a connaissance de sa malveillance.

Jusqu'à ce qu'un éditeur antivirus décide d'investir pour contrer le virus (attaque ciblée notamment).

Détection

Un malware n'est déclaré en tant que tel qu'à partir du moment où un ensemble de personnes ont indiqué que ce programme réalisait des choses qu'il ne devrait pas.

Ce dernier peut donc dormir au sein de votre ordinateur / smartphone / tablette / montre connectée... tant qu'un antivirus n'a connaissance de sa malveillance.

Jusqu'à ce qu'un éditeur antivirus décide d'investir pour contrer le virus (attaque ciblée notamment).

Lire les contrats.

Déclenchements

Quel pourrait-être le facteur déclenchant à une attaque virale ?

Déclenchements

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)

Déclenchements

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)

Déclenchements

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)
- Tâche planifiée

Déclenchements

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)
- Tâche planifiée
- Présence d'un élément déclencheur (fichier . . .)

Déclenchements

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)
- Tâche planifiée
- Présence d'un élément déclencheur (fichier . . .)
- Toc toc toc sur des ports réseaux

Déclenchements

Quel pourrait-être le facteur déclenchant à une attaque virale ?

- Démarrage (ordinateur, système, programme, raccourcis . . .)
- Horloge (Tchernobyl, date d'anniversaire)
- Tâche planifiée
- Présence d'un élément déclencheur (fichier . . .)
- Toc toc toc sur des ports réseaux
- . . .

Implantation

Où s'implante le malware ?

Implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)

Implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)

Implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)
- Au démarrage de Windows (clés de registre)

Implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)
- Au démarrage de Windows (clés de registre)
- Au démarrage d'un programme (processus enfant, dll malveillante)

Implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)
- Au démarrage de Windows (clés de registre)
- Au démarrage d'un programme (processus enfant, dll malveillante)
- À l'exécution d'un programme qui ne semblait pas être un malware

Implantation

Où s'implante le malware ?

- Au démarrage de l'ordinateur (BIOS / UEFI)
- Au démarrage du disque (MBR)
- Au démarrage de Windows (clés de registre)
- Au démarrage d'un programme (processus enfant, dll malveillante)
- À l'exécution d'un programme qui ne semblait pas être un malware
- ...

Gestation

- La gestation d'un malware est plus ou moins courte, cette phase peut-être réduite à 0 ou durer plusieurs mois, on parle alors de Command And Control (C&C).

Gestation

- La gestation d'un malware est plus ou moins courte, cette phase peut-être réduite à 0 ou durer plusieurs mois, on parle alors de Command And Control (C&C).
- Dans l'optique d'échapper à la surveillance des différents systèmes anti-malware, le virus va dialoguer au travers du réseau et se mettre à jour en changeant ainsi sa signature et s'adaptant.

Gestation

- La gestation d'un malware est plus ou moins courte, cette phase peut-être réduite à 0 ou durer plusieurs mois, on parle alors de Command And Control (C&C).
- Dans l'optique d'échapper à la surveillance des différents systèmes anti-malware, le virus va dialoguer au travers du réseau et se mettre à jour en changeant ainsi sa signature et s'adaptant.
- Durant ce temps de gestation, le malware a la possibilité de communiquer des informations sur son environnement ou *"simplement"* miner pour le compte de son propriétaire.

Nettoyage

- Après un temps indéterminé (plusieurs années parfois), les chercheurs en cybersécurité trouvent le malware et le signale donc aux éditeurs.

Nettoyage

- Après un temps indéterminé (plusieurs années parfois), les chercheurs en cybersécurité trouvent le malware et le signale donc aux éditeurs.
- Cependant, l'hôte n'en a pas pour le moins été infecté et même si l'antivirus indique avoir nettoyé le malware il est possible, voir probable que des éléments aient été corrompus.

Nettoyage

- Après un temps indéterminé (plusieurs années parfois), les chercheurs en cybersécurité trouvent le malware et le signale donc aux éditeurs.
- Cependant, l'hôte n'en a pas pour le moins été infecté et même si l'antivirus indique avoir nettoyé le malware il est possible, voir probable que des éléments aient été corrompus.
- Le système fonctionne donc correctement durant un certain temps mais peut-être avec un nouveau virus.

Prolifération

- Si le malware n'a pas été détecté, celui-ci peut-être programmé pour effectuer une attaque latérale.

Prolifération

- Si le malware n'a pas été détecté, celui-ci peut-être programmé pour effectuer une attaque latérale.
- Il va donc à son tour infecter les IOTs qui lui sont proches.

Prolifération

- Si le malware n'a pas été détecté, celui-ci peut-être programmé pour effectuer une attaque latérale.
- Il va donc à son tour infecter les IOTs qui lui sont proches.
- Et chaque IOT fera alors de même tant que l'infection ne sera pas stoppée.

Principales caractéristiques d'un malware

Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret

Principales caractéristiques d'un malware

Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué

Principales caractéristiques d'un malware

Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace

Principales caractéristiques d'un malware

Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent

Principales caractéristiques d'un malware

Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent
- Polymorphe

Principales caractéristiques d'un malware

Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent
- Polymorphe
- Malin

Principales caractéristiques d'un malware

Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent
- Polymorphe
- Malin
- ...

Principales caractéristiques d'un malware

Très difficile de donner des caractéristiques pour un malware cependant nous pourrions dire qu'il est :

- Discret
- Évolué
- Fugace
- Intelligent
- Polymorphe
- Malin
- ...

Quelle caractéristique informatique, abordée au début de cette présentation, permet la polymorphie du malware ?

No fake

Ces trois démonstrations sont issues d'attaques réelles.

No fake

Ces trois démonstrations sont issues d'attaques réelles.
"*Toute ressemblance avec des événements réels, passés ou présents, serait donc totalement naturelle.*"

Impression d'un document

Impression de documents *"maison"* au travail. . .

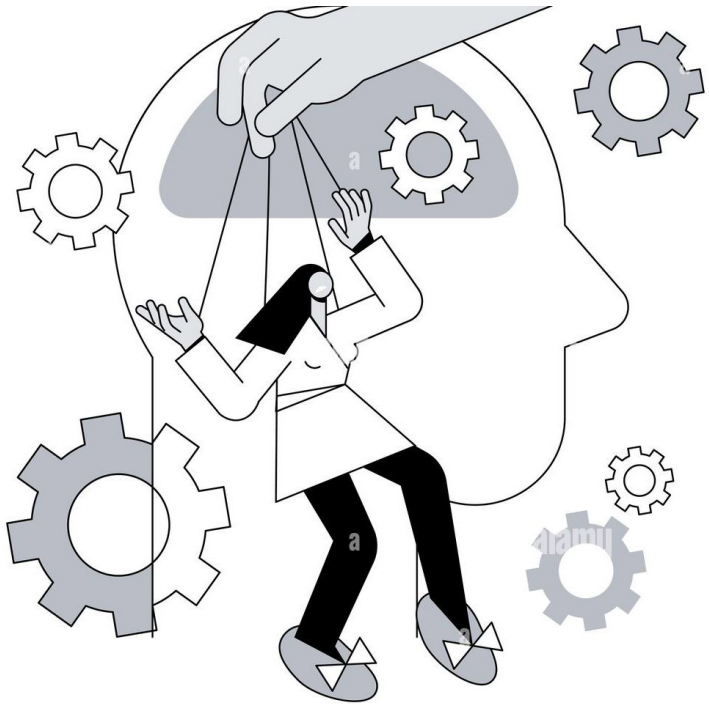
Téléchargement

Outre le fait que la plupart des cracks de logiciels contiennent des malwares cette attaque s'appuie sur l'ingénierie sociale.

Téléchargement

Outre le fait que la plupart des cracks de logiciels contiennent des malwares cette attaque s'appuie sur l'ingénierie sociale.

Démonstration



Téléchargement - Analyse

Reprenons :

1. L'usager visite une page "normale".

Téléchargement - Analyse

Reprenons :

1. L'usager visite une page "normale".
2. Un téléchargement d'un fichier zip est effectué de manière invisible.

Téléchargement - Analyse

Reprenons :

1. L'usager visite une page "normale".
2. Un téléchargement d'un fichier zip est effectué de manière invisible.
3. Triant le contenu de son dossier "Téléchargements", l'usager trouve un fichier Zip.

Téléchargement - Analyse

Reprenons :

1. L'usager visite une page "normale".
2. Un téléchargement d'un fichier zip est effectué de manière invisible.
3. Triant le contenu de son dossier "Téléchargements", l'usager trouve un fichier Zip.
4. Par **curiosité**, il dézippe le fichier.

Téléchargement - Analyse

Reprenons :

1. L'usager visite une page "normale".
2. Un téléchargement d'un fichier zip est effectué de manière invisible.
3. Triant le contenu de son dossier "Téléchargements", l'usager trouve un fichier Zip.
4. Par **curiosité**, il dézippe le fichier.
5. Une raccourci `.url` apparaît, il clique dessus par **curiosité**.

Téléchargement - Analyse

Reprenons :

1. L'usager visite une page "normale".
2. Un téléchargement d'un fichier zip est effectué de manière invisible.
3. Triant le contenu de son dossier "Téléchargements", l'usager trouve un fichier Zip.
4. Par **curiosité**, il dézippe le fichier.
5. Une raccourci `.url` apparaît, il clique dessus par **curiosité**.
6. Le poste est désormais compromis et contrôlable par l'attaquant.

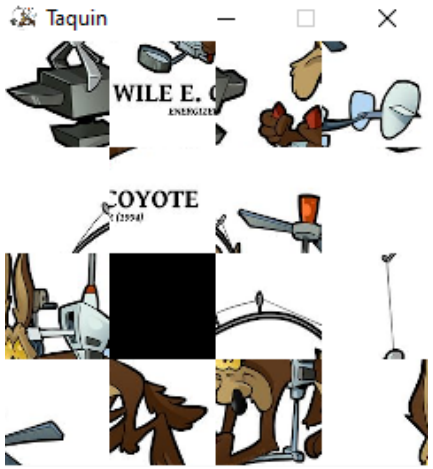
Exfiltration de données

Nouvelle technique d'ingénierie sociale : pour tromper l'EDR, l'IA ou l'antivirus, on exploite le comportement humain pour simuler un utilisateur légitime !

Exfiltration de données

Nouvelle technique d'ingénierie sociale : pour tromper l'EDR, l'IA ou l'antivirus, on exploite le comportement humain pour simuler un utilisateur légitime !

Démonstration



Comment me protéger ?

La meilleure protection est d'empêcher l'entrée du malware.

Comment me protéger ?

La meilleure protection est d'empêcher l'entrée du malware.

- Mise en place des bonnes pratiques (CIS Benchmarks PDFs).

Comment me protéger ?

La meilleure protection est d'empêcher l'entrée du malware.

- Mise en place des bonnes pratiques (CIS Benchmarks PDFs).
- Charte informatique associée à l'usage du système d'information et **notamment** des clés USBs et du télétravail.

Comment me protéger ?

La meilleure protection est d'empêcher l'entrée du malware.

- Mise en place des bonnes pratiques (CIS Benchmarks PDFs).
- Charte informatique associée à l'usage du système d'information et **notamment** des clés USBs et du télétravail.
- Contractualisation des interventions dans un contexte cyber.

Comment me protéger ?

La meilleure protection est d'empêcher l'entrée du malware.

- Mise en place des bonnes pratiques (CIS Benchmarks PDFs).
- Charte informatique associée à l'usage du système d'information et **notamment** des clés USBs et du télétravail.
- Contractualisation des interventions dans un contexte cyber.
- Se tester au travers de sensibilisations et de campagnes.

Comment me protéger ?

La meilleure protection est d'empêcher l'entrée du malware.

- Mise en place des bonnes pratiques (CIS Benchmarks PDFs).
- Charte informatique associée à l'usage du système d'information et **notamment** des clés USBs et du télétravail.
- Contractualisation des interventions dans un contexte cyber.
- Se tester au travers de sensibilisations et de campagnes.

Personnel formé,
système d'information protégé.

Rappelez-vous. . .

Si vous ne connaissez ni l'ennemi ni vous-même, vous succomberez à chaque bataille.

Sources

Images

- alamyimages.fr
- deviantart.com/koolaidman100x/art/Hacker-873230491
- fredcavazza.net
- pejac.es/indoor
- vrncomics.com
- warnerbros.com
- wysam.fr

Textes

- ChatGPT
- SunTzu

Inspiration

- Merci à tous les hackers de me donner chaque jour de nouveaux défis.